SOLUTION BRIEF

Fortinet and MistNet Security Solution

Broad, automated and integrated security with AI-driven SOC

Security Challenges

Infastructure Security

Lack of visibility into high-throughput and virtualized environments, and lack of understanding of traffic patterns can lead to missing detections of critical threats.

Threat Landscape

The attack surface is ever widening. With the long running attack scenarios and complicated multi-phase patterns, like insider threats, lateral movement attacks, zero-day malware, ransomware, and application attacks, many threat types are no longer detected using traditional tools.

Organizational Challenges

Security personnel are overwhelmed with the number of alerts from point solutions and find it difficult to upkeep the security infrastructure, often missing breaches or resulting in downtime.

The Fortinet and mistnet joint solution demonstrate how security and operations will be improved in different types of environment, from a small business to a power plant or a multinational corporation, by utilizing a joint approach of modern network security architecture meeting machine learning and AI to solve the security challenges stated above.

Joint Solution Benefits

- High-Speed Data collection
- Advanced multi-dimensional analytics for threat detection
- Entity (user and host), event contextualization
- Reductions of false-positives
- Shortened time-to-investigate and time-to-remediate
- Automated remediation
- Scalable event and log recording, storage, alerting

Joint Solution

MistNet AI-Driven SOC works together with Fortinet FortiGate Enterprise Firewall to look at the network traffic in order to find threats and provide visibility into the data flows. Security events and data patterns are analyzed using machine learning to find and stop single-vector attacks and multi-phased multivector advanced threats that are hard to detect otherwise.

Network Analytics, a component of mistnet's AI-Driven SOC, can be deployed as a hardware, virtual or container appliance in the datacenter or cloud to monitor traffic in the critical areas of the network using a tap or span from the network link. MistNet Network Analytics consumes FortiGate Enterprise Forewall logs to enrich network connection data with application and user context as well as threat logs for web, database, mobile, IoT security, etc.

Multiple security events are sent to the MistNet SOC Accelerator, second component of the SOC, for machine learning analysis and incident notification. SOC Accelerator presents a simple and concise incident report automating investigation tasks and remediation tasks performed by SOC Analysts through its integration with the Fortinet Security Fabric.

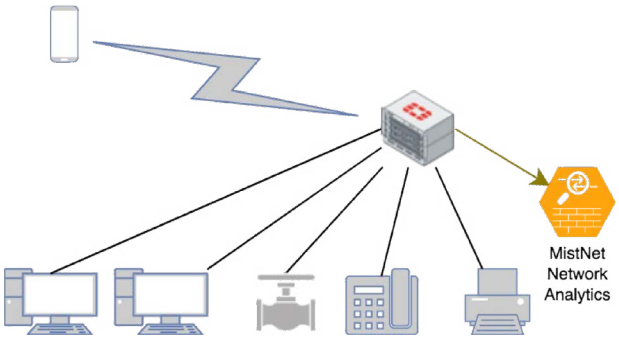

Figure 1: Fortinet and Mistnet Integration for AI-Driven SOC.

Use Case 1

MistNet and Fortinet reduce the SOC workload by learning expected event patterns and reducing the amount of falsepositives. Time-to-respond and time-to-remediate are greatly reduced by utilizing the context provided by FortiGate Enterprise Firewall and Security Fabric.

Visibility into the dark corners of the infrastructure is increased with the centralized monitoring and management combining Fortinet firewalls and MistNet sensors across the enterprise. In turn, the combined solution provides low total cost of ownership (TCO) by eliminating the need for managing and tuning disjoined security tools.

Mistnet AI-Driven SOC

Harnessing Machine Learning, Artificial Intelligence, MistNet's AI-Driven SOC solution empowers organizations by detecting and blocking threats in real-time as well as creating a rich record of all user, host and container transactions. The Fortinet and MistNet solution provides a high-performing and complete threat detection and investigative solution.

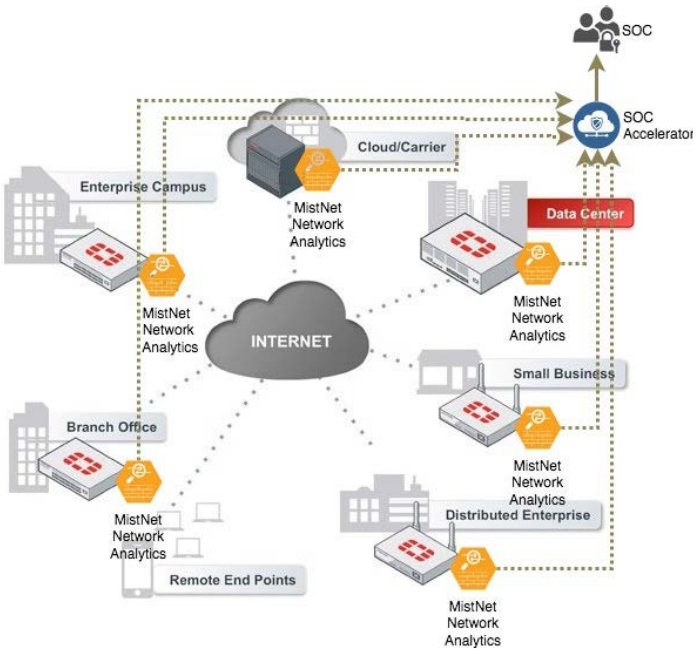

Figure 2: Multi-Site Integration.

Fortinet FortiGate Enterprise Firewall

FortiGate enterprise firewalls offer flexible deployments from the network edge to the core, data center, internal segment, and the Cloud. FortiGate enterprise firewalls leverages purpose-built security processors (SPUs) that delivers scalable performance of advanced security services like Threat Protection, SSL inspection, and ultralow latency for protecting internal segments and mission critical environments.

FortiGate NGFW provides automated visibility into cloud applications, IoT devices and automatically discovers end-to-end topology view of the enterprise network. FortiGate is a core part of security fabric and validated security protect the enterprise network from known and unknown attacks.

About MistNet

MistNet is revolutionizing cybersecurity with the world's first end-to-end AI driven Security Operations Center solution. MistNet combines real-time monitoring of all enterprise assets with advanced AI-based breach prevention. MistNet uses a comprehensive set of automated detection to prevent breaches that evade traditional defenses. Mistnet also detects and filters false positives to reduce the security operations cost and empowers security teams with an Enterprise DVR of all user and device activity. Deployed in major enterprise campuses, data centers and public clouds, customers benefit from comprehensive threat prevention, enhanced investigative capabilities and reduced false positives all in a single end-to-end solution.

June 20, 2019 1:28 AM

282353-A-0-EN

D:\Fortinet\Solution Brief\FA\GREY Solution Briefs\FA - SB - Fortinet MistNet\FA - SB - Fortinet MistNet